PCT/EP03/10327

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02020818.7

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02020818.7
Demande no:

Anmeldetag:
Date of filing: 17.09.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

SIEMENS AKTIENGESELLSCHAFT
Wittelsbacherplatz 2
80333 München
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

Beschreibung

Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen

Elektronische Signaturen werden verwendet, um Sicherheitsziele wie Authentizität, Verbindlichkeit und Integrität zu erreichen. Falls elektronische Daten als Willenserklärung interpretiert werden können, dient ein positives Ergebnis einer Prüfung einer elektronischen Signatur als Beweismittel für deren rechtliche Wirksamkeit. Elektronische Signaturen arbeiten mit zwei Schlüsseln, die gemeinsam erstellt und mathematisch voneinander abhängig sind. Einer dieser Schlüssel - nachfolgend privater Schlüssel - wird geheimgehalten und kann zur Erstellung einer elektronischen Signatur verwendet werden. Der andere Schlüssel - nachfolgend öffentlicher Schlüssel - wird veröffentlicht und kann zur Verifikation einer geleisteten Signatur verwendet werden. Um elektronische Signaturen Personen zuzuordnen, bedarf es einer Bindung des Namens einer Person an den entsprechenden öffentlichen Schlüssel. Diese Bindung erfolgt in der Form eines speziellen elektronischen Dokumentes, welches von einer vertrauenswürdigen dritten Instanz ausgestellt und als Zertifikat bezeichnet wird.

Technisch gesehen sind Zertifikate Datenstrukturen, die Informationen enthalten, mit denen eine Bindung von öffentlichen Schlüsseln an Schlüsselinhaber gewährleistet wird. Die konkrete Bindung eines öffentlichen Schlüssels an einen bestimmten Schlüsselinhaber wird durch eine vertrauenswürdige und neutrale Zertifizierungsstelle (CA - certification authority) vorgenommen, die das zugehörige vollständige Zertifikat mit ihrer elektronischen Signatur beglaubigt. Zertifikate haben nur eine begrenzte Gültigkeitsdauer, die ebenfalls als Bestandteil des Zertifikates von der Zertifizierungsstelle mitsigniert ist.

Die Zertifizierungsstelle übernimmt die Prüfung des Namens und bindet durch eine elektronische Signatur (mit ihrem privaten Schlüssel) den Namen der Person an den öffentlichen Schlüssel dieser Person. Das Resultat der Zertifizierung eines öffentlichen Schlüssels ist ein Zertifikat. Als Zertifikatsstruktur wird der Standard X.509 benutzt. Solch ein Zertifikat umfaßt neben dem öffentlichen Schlüssel den Namen der ausstellenden Zertifizierungsstelle, einen Gültigkeitszeitraum, den Namen des Eigentümers und eine eindeutige Nummer der ausstellenden Zertifizierungsstelle. Hierbei wird vorausgesetzt, daß alle beteiligten Personen dem öffentlichen Schlüssel dieser Zertifizierungsstelle vertrauen. Zertifizierungsstellen besitzen getrennte Schlüsselpaare für das Signieren von Zertifikaten, Sperrlisten und Zeitstempeln sowie für die Abwicklung der Kommunikation mit anderen Kommunikationspartnern.

Bekannte Signaturverfahren bestehen aus einem Algorithmus zur Erzeugung elektronischer Signaturen und einem zugeordneten Algorithmus zur Verifikation elektronischer Signaturen. Die elektronischen Daten, für die eine elektronische Signatur gebildet wird, werden üblicherweise als Anhang den elektronisch signierten Daten beigefügt. Jeder Algorithmus zur Erzeugung elektronischer Signaturen erhält als Eingangsparameter zumindest zu signierende Daten sowie einen privaten Schlüssel eines Unterzeichners und liefert als Ergebnis eine elektronische Signatur. Der zugeordnete Algorithmus zur Verifikation elektronischer Signaturen erhält als Eingangsparameter zumindest elektronisch signierte Daten sowie einen öffentlichen Schlüssel eines Unterzeichners und liefert ein positives oder negatives Verifikationsergebnis, je nach dem, ob die Verifikation erfolgreich war.

Eine Erzeugung elektronischer Signaturen erfolgt bisher entsprechend nachstehender Reihenfolge:

- Erzeugung eines asymmetrischen Schlüsselpaars mit einem privaten und einem öffentlichen Schlüssel,

- Ausstellung eines Zertifikats für den öffentlichen Schlüssel,
- Bestimmung eines Hashwertes für die zu signierenden Daten,
- Berechnung der elektronischen Signatur durch Anwendung einer vorgegebenen Signaturfunktion,
- Ausgabe der elektronischen Signatur.

Eine Verifikation elektronischer Signaturen erfolgt bisher entsprechend nachstehender Reihenfolge:

- Bestimmung eines Hashwertes der elektronischen Daten aus dem Anhang zur elektronischen Signatur,
- Anwendung einer vorgegebenen Verifikationsfunktion auf die elektronische Signatur und den Hashwert,
- Ausgabe des Verifikationsergebnisses.

Signaturverfahren unterscheiden sich durch die verwendete Signatur- und Verifikationsfunktion (z.B. RSA, DSA oder ECDSA), einen verwendeten Hashalgorithmus zur Bestimmung des Hashwertes (z.B. SHA-1 oder RIPEMD-160) und ein ggf. verwendetes Paddingverfahren (bei RSA). Ein Paddingverfahren wird angewendet, um einen Hashwert durch eine vorgebbare Zeichenkette zu ergänzen, falls eine Anpassung der Länge des Hashwertes erforderlich ist.

Bisher bekannten Signaturverfahren ist ein hoher Aufwand zur dauerhaften Sicherung des privaten Signaturschlüssels auf Seiten der Person, welcher der private Signaturschlüssel zugeordnet ist, gegen unberechtigten Zugriff gemeinsam.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde ein Verfahren zur Erzeugung von elektronischen Signaturen zu schaffen, das keine dauerhafte Sicherung eines privaten Signaturschlüssels auf Seiten einer Person, welcher der private Signaturschlüssel zugeordnet ist, gegen unberechtigten Zugriff erfordert.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens sind in den abhängigen Ansprüchen angegeben.

Ein wesentlicher Aspekt der vorliegenden Erfindung besteht darin, daß eine Zertifizierung eines öffentlichen Validierungsschlüssels erst nach einer Berechnung einer elektronischen Signatur erfolgt. Eine willentliche, durch ein signiertes Dokument ausgedrückte Handlung seitens eines Verfasser eines elektronischen Dokuments erfolgt somit erst nach Signaturgenerierung im Rahmen eines Zertifikatsbeantragungsprozesses. Da nicht eine Veranlassung einer Berechnung einer elektronischen Signatur, sondern eine Zertifikatsbeantragung die willentliche Handlung darstellt, ist es nicht erforderlich, einen zum öffentlichen Validierungsschlüssel korrespondierenden privaten Signaturschlüssel nach Berechnung der elektronischen Signatur aufzubewahren. Daher kann der private Signaturschlüssel nach Berechnung der elektronischen Signatur vernichtet werden und muß daher nicht mehr gegen unberechtigten Zugriff gesichert werden.

Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert. Es zeigt

Figur 1 eine Darstellung eines Ablaufs eines herkömmlichen Signaturverfahrens,

Figur 2 - eine Darstellung eines Ablaufs eines erfindungsgemäßen Signaturverfahrens.

In Figur 1 ist ein Ablauf eines herkömmlichen Signaturverfahrens dargestellt, bei dem zunächst ein Schlüsselpaar generiert wird, das einen privaten Signaturschlüssel 110 und einen öffentlichen Validierungsschlüssel umfaßt (Schritt 100). Nachfolgend wird ein Zertifikatsantrag bei einer Registrierungsstelle 112 (RA - registration authority) gestellt

(Schritt 101). Im Zusammenspiel zwischen der Registrierungsstelle 112 und einer Zertifizierungsstelle 113 (CA - certification authority) wird eine Identitätsprüfung in Bezug auf einen jeweiligen Antragssteller vorgenommen (Schritt 102).

Bei einem positiven Überprüfungsergebnis vergibt die Zertifizierungsstelle 113 ein Zertifikat für den öffentlichen Validierungsschlüssel an einen jeweiligen Antragssteller (Schritt 103) und speichert einen entsprechenden Eintrag für das ausgegebene Zertifikat in einer der Zertifizierungsstelle 113 zugeordneten Datenbasis 114 ab, die zur Zertifikatsabfrage öffentlich zugänglich ist. Außerdem sind in der Datenbasis 114 Zertifikatssperrlisten gespeichert, die über ungültige Zertifikate informieren. Nach Zertifizierung des öffentlichen Validierungsschlüssels wird für ein zu signierendes elektronisches Dokument 111 eine elektronische Signatur unter Verwendung des privaten Signaturschlüssels 110 und einer vorgebbaren Signaturfunktion berechnet (Schritt 104). Anschließend werden die berechnete Signatur und das elektronische Dokument 111 über einen Nachrichtenkanal vom Verfasser des elektronischen Dokuments 111 als Nachricht an einen Empfänger des elektronischen Dokuments 111 übertragen (Schritt 105).

Empfängerseitig wird zur Validierung der elektronischen Signatur eine Zertifikatsabfrage noch vorgenommen (Schritt 106). Dabei wird entweder ein dem Verfasser zugeordneter öffentlicher Validierungsschlüssel aus der Datenbasis 114 abgefragt, oder es wird ein dem in der übertragenden Nachricht enthaltenen öffentlichen Validierungsschlüssel zugeordneter Eintrag in der Datenbasis 114 abgefragt, der ggf. die Gültigkeit des zugeordneten Zertifikats bestätigt. Abschließend wird eine Validierung der in der übertragenen Nachricht enthaltenen Signatur durch den Empfänger vorgenommen (Schritt 107). Bei der Validierung der elektronischen Signatur durch den Empfänger wird einerseits die Signatur mit Hilfe des öffentlichen Validierungsschlüssels entschlüsselt und andererseits ein Hash-Wert für das elektronische Dokument 111 berechnet. Ab-

schließend werden die entschlüsselte Signatur und der berechnete Hash-Wert auf Übereinstimmung verglichen. Bei Übereinstimmung der entschlüsselten Signatur und des berechneten Hash-Wertes wird die Signatur empfängerseitig als gültig anerkannt.

In Figur 2 ist ein Ablauf eines erfindungsgemäßen Signaturverfahrens dargestellt, bei dem zunächst ein asymmetrisches Schlüsselpaar erzeugt wird (Schritt 200). Mittels eines vom generierten Schlüsselpaar umfaßten privaten Signaturschlüssels 210 und einer vorgebbaren Signaturfunktion wird aus einem elektronischen Dokument 211 verfasserseitig eine elektronische Signatur berechnet (Schritt 201). Nach Berechnung der elektronischen Signatur wird diese durch den Verfasser validiert, um sicherzustellen, daß die berechnete elektronische Signatur einer durch das elektronische Dokument 111 ausgedrückten Willenshandlung entspricht (Schritt 202).

Bei einem positiven Validierungsergebnis wird ein Zertifikat für einen zum privaten Signaturschlüssel 210 korrespondierenden öffentlichen Validierungsschlüssel bei einer Registrierungsstelle 212 beantragt (Schritt 203). Nachfolgend werden im Zertifikatsantrag enthaltene Angaben überprüft, insbesondere die Identität des Verfassers bzw. eines Antragsstellers (Schritt 204).

Bei einem positiven Überprüfungsergebnis wird von einer Zertifizierungsstelle 213 ein Zertifikat für den öffentlichen Validierungsschlüssel an den Antragssteller bzw. Verfasser des elektronischen Dokuments 211 ausgegeben (Schritt 205). Außerdem wird ein entsprechender Eintrag in einer der Zertifizierungsstelle 213 zugeordneten Datenbasis für das ausgegebene Zertifikat vorgenommen.

Nach Validierung der berechneten Signatur durch den Verfasser des elektronischen Dokuments 211 und nach Zertifizierung des öffentlichen Validierungsschlüssels werden das elektronische

Dokument 211 und die berechnete elektronische Signatur als Nachricht zu einem Empfänger des elektronischen Dokuments 211 über einen Nachrichtenkanal übertragen (Schritt 206). Empfängerseitig wird in bekannter Weise eine Zertifikatsabfrage vorgenommen (Schritt 207) und eine Validierung der in der empfangenen Nachricht enthaltenen Signatur durchgeführt (Schritt 208).

Bei der Validierung einer elektronischen Signatur werden nur solche Signaturen als gültig anerkannt, die zu einem Zeitpunkt vor der Zertifizierung des öffentlichen Validierungsschlüssels erzeugt wurden. Hierdurch entfällt die bei bisherigen Signaturverfahren bekannte Revokationsproblematik in bezug auf öffentliche Validierungsschlüssel. Außerdem kann auf diese Weise nach dem Zeitpunkt der Zertifizierung des öffentlichen Validierungsschlüssels kein Mißbrauch mehr mit dem privaten Signaturschlüssel betrieben werden, so daß keine Mechanismen zur dauerhaften Vermeidung unberechtigter Zugriffe auf den privaten Signaturschlüssel 210 erforderlich sind.

Bei der Zertifizierung des öffentlichen Validierungsschlüssels entsprechend den Schritten 203 bis 205 kann zusätzlich zu einem Benutzeridentifikator und dem öffentlichen Validierungsschlüssel eine Referenz auf das jeweils signierte elektronische Dokument 211 einbezogen werden. Bei der empfängerseitigen Validierung der Signatur gemäß Schritt 208 wird dann die Referenz zum elektronischen Dokument 211 zusätzlich ausgewertet. Darüber hinaus ist es möglich, nicht nur eine Referenz auf ein einziges elektronisches Dokument in die Zertifizierung des öffentlichen Validierungsschlüssels einzubeziehen, sondern eine Mehrzahl von Referenzen auf innerhalb eines bestimmten Bezugszeitraumes signierte elektronische Dokumente. Eine Referenz auf ein elektronisches Dokument wird beispielsweise durch eine Berechnung eines Hash-Wertes für das jeweilige elektronische Dokument implementiert. Bei einer empfängerseitigen Validierung der Signatur entsprechend

Schritt 208 werden dann die entsprechenden Hash-Werte miteinander verglichen.

Eine Anwendung des erfindungsgemäßen Signaturverfahrens ist beispielsweise innerhalb eines zentralen Hardware-Sicherheitsmoduls möglich. Hierbei steht sämtlichen Mitgliedern einer geschlossenen Benutzergruppe ein privater Signaturschlüssel im zentralen Hardware-Sicherheitsmodul gemeinsam zur Verfügung. Benutzerseitig werden Hash-Werte für zu signierende elektronische Dokumente erzeugt und über einen geschützten Übertragungskanal an das Hardware-Sicherheitsmodul übermittelt. Das Hardware-Sicherheitsmodul berechnet ohne weitere Überprüfung die elektronische Signatur und sendet diese zurück einen jeweiligen Benutzer. Der jeweilige Benutzer speichert das signierte elektronische Dokument mit zugehörigem Hash-Wert und elektronischer Signatur nach erfolgreicher Validierung der Signatur durch den jeweiligen Benutzer ab. Die zugehörigen Hash-Werte werden zu einem späteren Zeitpunkt dem Zertifikatsantrag für den öffentlichen Validierungsschlüssel beigefügt und durch die Zertifizierungsstelle im Zertifikat für den öffentlichen Validierungsschlüssel als zusätzliches Attribut inkludiert. Das Zertifikat ist damit in eindeutiger Weise mit dem signierten elektronischen Dokument verknüpft.

Anstelle einer Nutzung eines zentralen Hardware-Sicherheitsmoduls ist auch eine Nutzung eines persönlichen Sicherheitsmoduls zur Signaturerzeugung möglich. Dabei wird der Hash-Wert für das zu signierende elektronische Dokument beispielsweise an einem Personal Computer o.ä. erzeugt und über eine Infrarot- oder Bluetooth-Schnittstelle an das persönliche Sicherheitsmodul übermittelt.

Eine weitere Anwendung des erfindungsgemäßen Signaturverfahrens besteht in einer Nutzung eines modifizierten und mit einer Validierungslogik versehenen Druckers. Als Eingangsparameter erhält ein solcher Validierungsdrucker ein zu signierendes elektronisches Dokument und eine für dieses elektroni-

sche Dokument berechnete elektronische Signatur. Bei erfolgreicher Validierung der elektronischen Signatur wird das zugehörige elektronische Dokument auf dem Validierungsdrucker ausgegeben. Anschließend wird dem Verfasser des elektronischen Dokuments die Möglichkeit geboten anhand des Ausdrucks zu entscheiden, ob er den zuvor verwendeten privaten Signaturschlüssel zertifizieren lassen will.

Die Anwendung der vorliegenden Erfindung ist nicht auf die hier beschriebenen Ausführungsbeispiele beschränkt.

Patentansprüche

1. Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen, bei dem
- ein asymmetrisches Schlüsselpaar erzeugt wird, das einen privaten Signaturschlüssel und einen öffentlichen Validierungsschlüssel umfaßt,
- zumindest eine elektronische Signatur mittels des privaten Signaturschlüssels und durch Anwendung einer vorgebbaren Signaturfunktion für zumindest ein elektronisches Dokument berechnet wird,
- nach Berechnung der zumindest einen elektronischen Signatur eine Zertifizierung des öffentlichen Validierungsschlüssels erfolgt.

2. Verfahren nach Anspruch 1, bei dem
bei einer Validierung nur Signaturen als gültig erkannt werden, die zu einem Zeitpunkt vor der Zertifizierung des öffentlichen Validierungsschlüssels erzeugt werden und/oder wurden.

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem
bei der Zertifizierung des öffentlichen Validierungsschlüssels zusätzlich zu einem Benutzeridentifikator und dem öffentlichem Validierungsschlüssel zumindest eine Referenz auf das zumindest eine elektronische Dokument einbezogen wird.

4. Verfahren nach Anspruch 3, bei dem
eine Implementierung der zumindest einen Referenz durch eine Berechnung eines Hash-Wertes für das zumindest eine elektronische Dokument erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem
nach Berechnung der Signatur und vor deren Übermittlung an einen Empfänger eine Validierung durch einen Verfasser des zumindest einen elektronischen Dokuments zur Überprüfung ei-

ner durch das zumindest eine elektronische Dokument ausgedrückten Willenshandlung erfolgt.

Zusammenfassung

Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen

Die Erfindung betrifft ein Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen, bei dem ein asymmetrisches Schlüsselpaar erzeugt wird, das einen privaten Signaturschlüssel und einen öffentlichen Validierungsschlüssel umfaßt. Außerdem wird zumindest eine elektronische Signatur mittels des privaten Signaturschlüssels und durch Anwendung einer vorgebbaren Signaturfunktion für zumindest ein elektronisches Dokument berechnet. nach Berechnung der zumindest einen elektronischen Signatur erfolgt eine Zertifizierung des öffentlichen Validierungsschlüssels.

Figur 2

Fig. 2

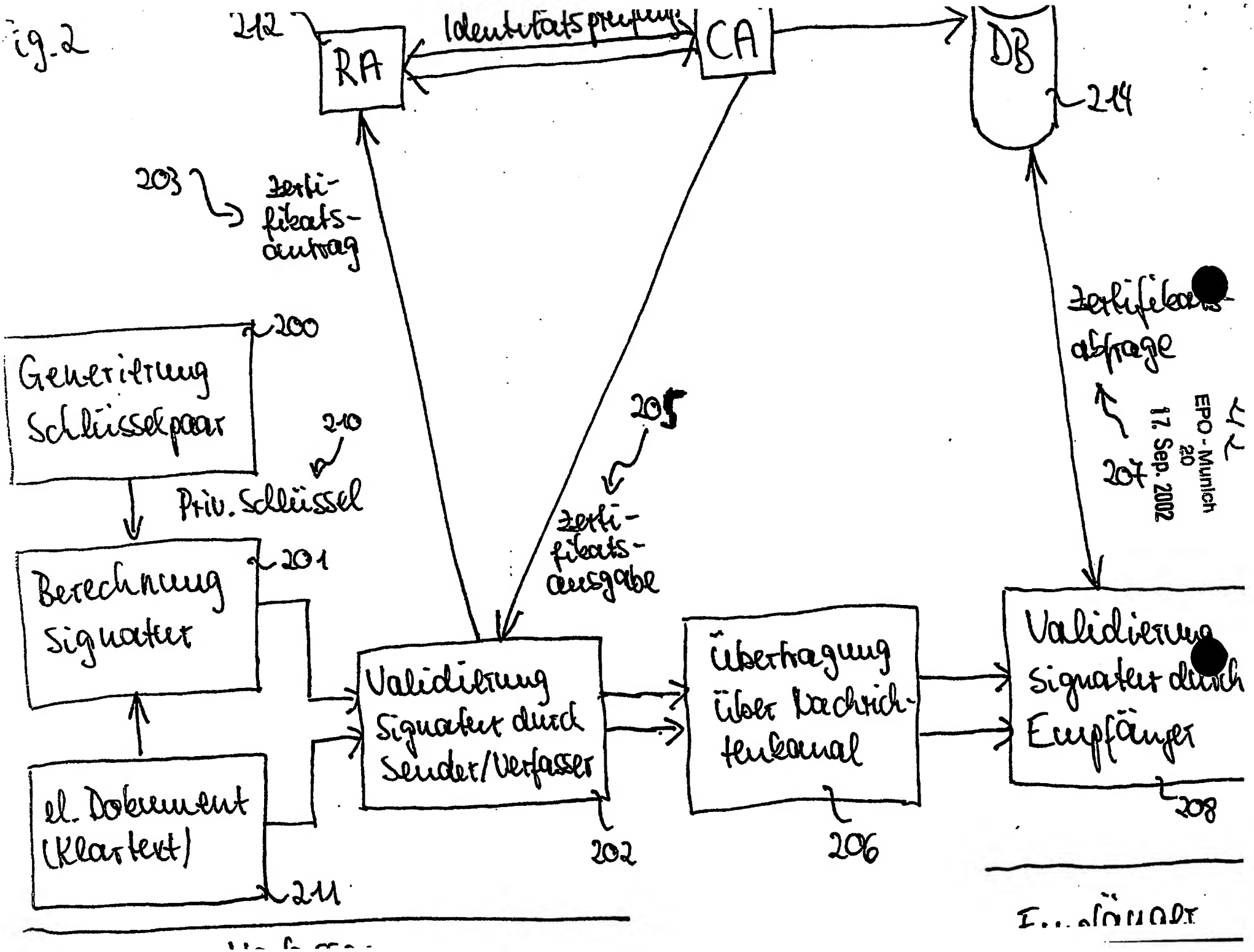


Fig. 1
(nach der Technik)

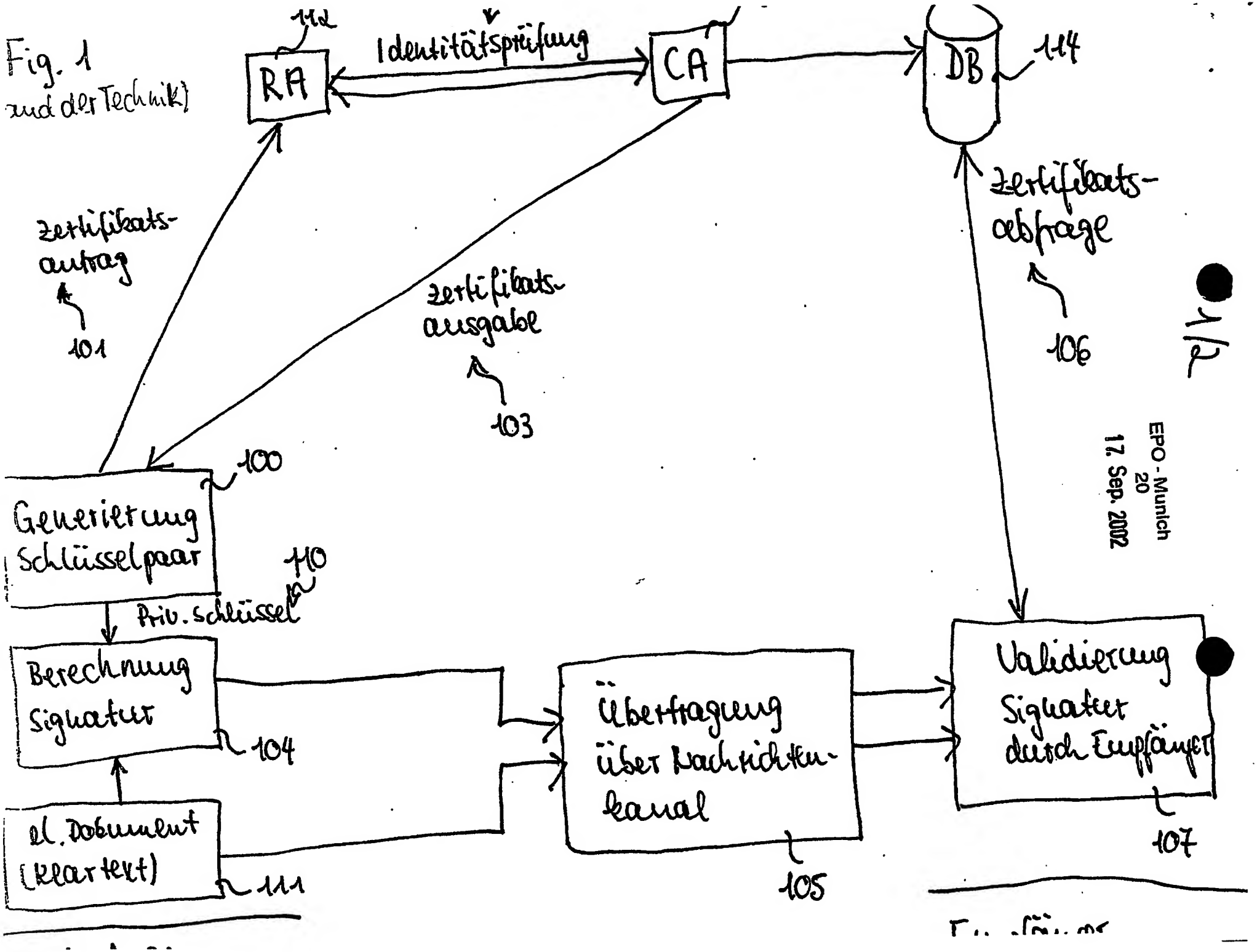
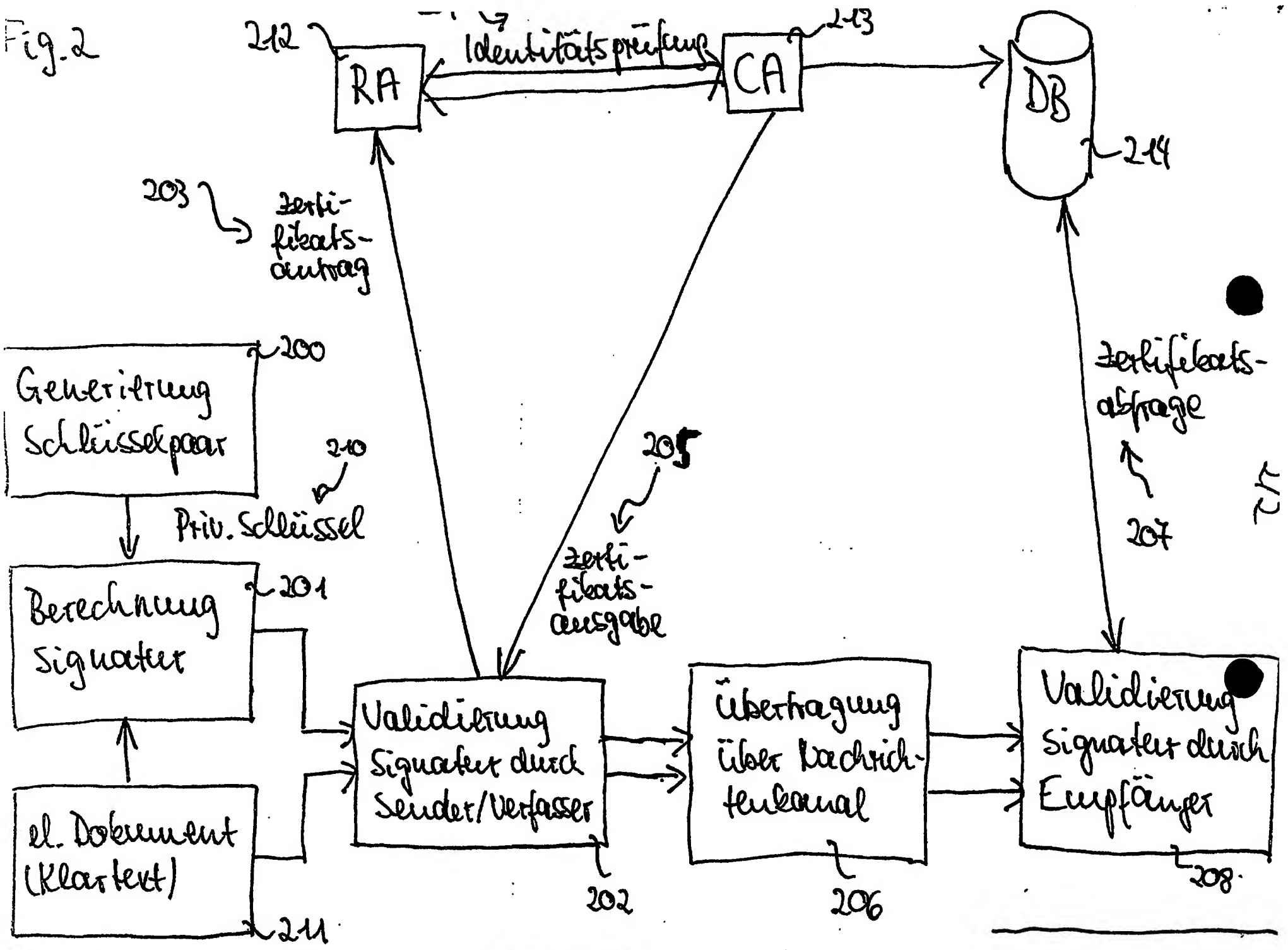


Fig. 2


212
RA
Identitätsprüfung
CA
213
DB
214
203
Zertifikats-antrag
200
Generierung Schlüsselpaar
210
Priv. Schlüssel
205
Zertifikats-ausgabe
Zertifikats-abfrage
207
201
Berechnung Signatur
Validierung Signatur durch Sender/Verfasser
202
Übertragung über Nachrichtenkanal
206
Validierung Signatur durch Empfänger
208
el. Dokument (Klartext)
211